(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 658 054 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
16.09.1998 Bulletin 1998/38

(51) Int Cl.6: **H04N 7/16**, H04N 7/167

(21) Application number: **94119403.7**

(22) Date of filing: **08.12.1994**

(54) **Apparatus and method for securing communication systems**

Gerät und Verfahren zur Sicherung von Kommunikationssystemen

Appareil et méthode de protection des systèmes de communication

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **09.12.1993 IL 10796793**

(43) Date of publication of application:
14.06.1995 Bulletin 1995/24

(73) Proprietor: **NEWS DATACOM LTD.**
London E1 9XY (GB)

(72) Inventors:
- **Nachman, Jacob Bezalel**
  Ramat Modiim 73127 (IL)
- **Tsuria, Yossef**
  Jerusalem 97276 (IL)

(74) Representative: **Modiano, Guido, Dr.-Ing. et al**
Modiano, Josif, Pisanty & Staub,
Baaderstrasse 3
80469 München (DE)

(56) References cited:
EP-A- 0 343 805
EP-A- 0 438 154
EP-A- 0 588 184
WO-A-85/00491
WO-A-91/11884

- **BBC RESEARCH DEPARTMENT REPORT, no. 10, August 1988 TADWORTH, SURREY, GR.BRITAIN, pages 1-18, D.T.WRIGHT 'CONDITIONAL ACCES BROADCASTING: DATDCARE 2'**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 0 658 054 B1

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

The present invention relates generally to secure communication systems and more particularly to systems wherein encrypted information is transmitted from a single location to multiple terminals located at non-secure locations.

BACKGROUND OF THE INVENTION

A major problem in secure communication systems is the possibility of unauthorized penetration. Unauthorized penetration of this kind is referred to as hacking.

Several methods have been employed to overcome the problem of hacking. Encryption of transmitted data and authentication of communicators are some of the methods employed to make hacking more difficult.

One hacking method which is considered difficult to overcome is called "The McCormac Hack". This method, which is believed to be theoretically applicable to CATV systems, is described in the book "World Satellite TV and Scrambling Methods", 2nd Edition, Baylin Publications 1991, pp. 242 - 244 by Frank Baylin, Richard Maddox and John McCormac and in "Satellite Watch News", August 1991. According to this method, a data stream from a legitimately authorized decoder, is extracted in real time and transmitted over the air using a small radio-frequency (RF) transmitter. The data stream is then used to activate a number of pirate decoders.

WO-A-91 11884 describes a decoder for descrambling encoded satellite transmission. The decoder receives twice-encrypted keys and performs a first key decryption in a first removable module in accordance with a secret serial number stored in the first removable module. The partially decrypted key of the first removable module is supplied to a second decryptor where the key is fully decrypted using a further secret serial number stored in the second decryptor. The arrangement according to WO-A-91 11884 ensures that the replaceable module operates only on a particular decoder to which the replaceable module has been assigned.

EP-A-343 805 teaches the reproduction of secure keys by using distributed key generation data.

SUMMARY OF THE INVENTION

The present invention seeks to provide a system and a method which substantially prevent the possibility of extracting a data stream from a legitimately authorized terminal and transmitting the data stream to a plurality of pirate terminals.

For the purposes of the present invention, the term "terminals" in all of its forms is used in a broader than usual sense to cover all types of computer terminals, CATV decoders, remote computers and remote computerized stations.

For the purposes of the present invention, the terms "seed" and "key" in all of their forms are alternately used in a broader than usual sense to cover all types of numbers or other symbols, either secret or non-secret, which are used at least as part of encryption/decryption keys to encrypt/decrypt (or scramble/descramble) data. The term "secret number" will be further used, for the purpose of the present invention, to denote the secret key which is used for encryption/decryption (or scrambling/descrambling) of data.

There is thus provided in accordance with a preferred embodiment of the present invention a hacking prevention system or method for use with a network including a transmitter and a multiplicity of receivers as set out in the independent claims 1 and 14.

Preferred embodiments of the invention are set out in dependent claims 2 - 13 and 15.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a generalized block diagram illustration of a theoretical hacking system based on the prior art "McCormac Hack" method;

Fig. 2 is a generalized block diagram illustration of part of a subscriber unit constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is a flowchart description of the functionality of the apparatus of Fig. 2;

Fig. 4 is a flowchart description of the functionality of the apparatus of Fig. 2 in accordance with an alternative embodiment of the invention which does not employ conditional access cards;

Fig. 5 is a generalized block diagram illustration of part of a subscriber unit in accordance with a preferred embodiment of the invention in which receivers characterized by different parameters are enabled with the same secret number; and

Fig. 6 is a flowchart description of the functionality of the apparatus of Fig. 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1, which is a generalized block diagram illustration of a theoretical hacking system constructed and operative in accordance with the prior art "McCormac Hack" method.

An authorized decoder 10, which is normally operated by a valid smart card 12, is coupled instead to a McCormac's Hack Interface (MHI) unit 14 via a standard smart card communication link 15. Smart card 12 is also coupled to the MHI unit 14 via a standard smart card communication link 16.

MHI unit 14 "sniffs" the communication data passed between the smart card 12 and the authorized decoder 10 and provides it to a small radio transmitter 18. Radio transmitter 18 transmits the data via a radio-frequency (RF) link 19 to a radio receiver 20 which is coupled to a virtual smart card unit 22. Virtual smart card unit 22 is coupled to an unauthorized decoder 24 via a standard smart card communication link 25. In this way the unauthorized decoder 24 is operated by the same data stream that operates the authorized decoder 10.

In an alternative embodiment, MHI unit 14 "sniffs" the data which is communicated between units inside the authorized decoder 10. In this embodiment, MHI unit 14 is linked, via communication link 27, to a communication BUS 26 extending between a micro-processor 28 and a descrambling device 29. Communication BUS 26 carries the "seed" value which is the secret number required for descrambling. In this way the seed value may be extracted and transmitted to the unauthorized decoder for descrambling of the data.

Reference is now made to Fig. 2, which is a generalized block diagram illustration of part of a subscriber unit constructed and operative in accordance with a preferred embodiment of the present invention.

In accordance with a preferred embodiment of the present invention, a data stream including a series of authorization packets PKT1,...,PKTn is transmitted from an information source via a satellite link, to a packet receiver and descrambler unit 30 which forms part of a subscriber's CATV receiver and decoder (not shown). A series of offset values DELTA1,...,DELTAn is also transmitted via the satellite link and received by the packet receiver and descrambler unit 30. Preferably, each packet is paired with an offset value.

In the packet receiver and descrambler unit 30 a Packet Receiver Unit (PRU) 32 receives the series of packets and the offset values. A random number generator 34 provides a number in the range 1,...,n to PRU 32 by employing a random number algorithm. According to the selected number, for example 3, the corresponding packet, i.e. PKT3, is transmitted to a smart card 36 and a corresponding offset value, i.e. DELTA3, which serves as an internal key, is transmitted to a descrambler unit 38.

Smart card 36 employs an algorithm which produces an appropriate seed for each packet. When smart card 36 receives PKT3 it produces a corresponding key, here termed SEED3, and provides it to the descrambler unit 38.

It is to be appreciated that PRU 32, random number generator 34 and the descrambler unit 38 are all embodied in a secure chip such as a VLSI chip. Thus, the communication of the random number and the offset value cannot be altered or "sniffed".

In the descrambler unit 38 the keys DELTA3 and SEED3 received from PRU 32 and smart card 36 respectively are employed by a function f such that:

(1) f=f(seed value, offset value), and

(2) SEED0 = f(SEEDi,DELTAi) for any i=1,..., n,

where SEED0 is the secret number required for descrambling of the data and "i" is any integer value in the series 1,...,n. If the value i=3 is selected then:

(3) SEED0 = f(SEED3,DELTA3).

In accordance with a preferred embodiment of the present invention, the descrambler 38 functions as a secret number generator in generating the SEED0 value and also functions as a key receiver, which receives an internal key and a key from the smart card. The SEED0 value is employed by the descrambler 38 for descrambling of the data. Inasmuch as the descrambler 38 is in a VLSI format it is considered difficult, if not practically impossible, to tap the SEED0 value.

It is to be appreciated that the hacking prevention system of Fig. 2 may be also operable with systems which do not employ smart cards. In that case the seed values corresponding to the packets PKT1,...,PKTn may be calculated and produced in any suitable part of the packet receiver and descrambler 30, such as, for example, any one of PRU 32, random number generator 34 and descrambler 38, by employing an algorithm which is similar to the one employed in the smart card. Upon receipt of the selected random number from random number generator 34, the corresponding calculated seed value and the appropriate offset value are provided to descrambler unit 38.

Reference is now made to Fig. 3 which is a flowchart description of the functionality of the apparatus of Fig. 2.

A series of data packets PKT1,...,PKTn and a series of offset values DELTA1,...,DELTAn are received via a satellite link. A random number generation algorithm is employed to calculate and select one of the index numbers 1,...,n. The output of the random number generation algorithm is, for example the index 3. The packet whose index number was calculated, i.e. PKT3, is transmitted to the smart card. In the smart card an algorithm which calculates seeds is employed to calculate the corresponding SEED3 number. SEED3 is then transmitted to descrambler unit 38.

The offset value which corresponds to the calculated index number, i.e. DELTA3, is transmitted to the descrambling unit 38 where it is combined or otherwise utilized, by use of a secret number generator, with SEED3, to calculate a SEED0 value which is the secret number employed to descramble the satellite transmissions.

Reference is now made to Fig. 4 which is a flowchart description of the functionality of the apparatus of Fig. 2 according to an alternative embodiment of the invention. The flowchart of Fig. 4 is similar to the one described in Fig. 3 except that the calculation of the seeds is not performed in a smart card but rather in PRU 32 of Fig. 2. It is to be appreciated that the calculation of the seeds is not limited to PRU 32 but may rather be performed in any part of the secure VLSI chip which forms the packet receiver and descrambler unit 30 shown in Fig. 2.

Reference is now made to Fig. 5 which is a generalized block diagram illustration of part of a subscriber unit in accordance with a preferred embodiment of the invention in which receivers of information supplied by different suppliers or receivers which are otherwise distinguished from each other, as by demographics, geographic location or any other parameter, are enabled with the same secret number.

The system of Fig. 5 is similar to the system of Fig. 2 except that additional data is received from an information source via the satellite link and processed in a packet receiver and descrambler unit 130.

PRU 132 rèceives, via a satellite link, the following data: a series of packets PKT1,...,PKTn; a series of first offset values DELTA1,...,DELTAn to be employed in part of the abovementioned anti-hacking method; and a series of second offset values GAMMA1,..., GAMMAk.

The series of second offset values GAMMA1,..., GAMMAk is employed to distinguish between separate groups of subscribers/receivers which may be distinguished from each other on the basis of one or more criteria, such as their program suppliers, their geographic location or their demographics. Thus, each group of receivers is characterized by one of the second offset values.

Characterization of the group of receivers can be achieved either by an internal code or an internal algorithm which is entered during manufacture of each decoder, preferably in packet receiver and descrambler 130, or by an algorithm in the smart card which upon its first communication with the decoder causes the decoder to be valid for a selected parameter or group of parameters, as exemplified above. Thus, upon such characterization, each decoder is enabled to select only one of the second offset values GAMMA1,...,GAMMAk.

Alternatively or additionally the characterization of the decoder may be achieved using only the first offset values. In such a case, different decoders may be set to receive only certain ones of the offset values and not others. In this way, the use of the second offset values may be obviated.

If, for example, the decoder is characterized to select GAMMA2, which defines a unique program supplier, PRU 132 will transmit GAMMA2 to descrambler unit 138. Upon selection of a random number, for example 3, by random number generator 134, PRU 132 transmits the respective data packet PKT3 to smart card 136. PRU 132 also transmits an offset value from the series of offset values DELTA1,...,DELTAn according to the selected random number, i.e. DELTA3, to descrambler unit 138.

When issued, the set of smart cards for the subscribers for each group are different from the set of smart cards issued for the subscribers of another group. Differentiation is achieved by employing different algorithms in each set of smart cards. Therefore, for example, even if in two decoders, which are operated by two different information suppliers, the same random number is selected, i.e. 3, and the same data packet is transmitted to both smart cards, i.e. PKT3, each smart card calculates a different seed value, i.e. SEED3 and SEED3*.

Since each of the abovementioned two decoders is operated by a separate program supplier, different second offset values area transmitted to descrambler unit 138, for example GAMMA2 and GAMMA3 respectively.

In the descrambler units 138 of the two decoders the same secret number generator is operated such that:

(4) f=f(seed value, first offset value, second offset value);

(5) SEED0 = f(SEED3, DELTA3, GAMMA2); and also

(6) SEED0 = f(SEED3*, DELTA3, GAMMA3).

It is to be appreciated that in accordance with the abovementioned method the same SEED0 may be employed for descrambling of information originated from one source and targeted to separate groups of subscribers while preventing subscribers of one group from receiving intelligible information destined for another group.

Reference is now made to Fig. 6 which is a flowchart description of the functionality of the apparatus of Fig. 5.

A series of data packets PKT1,...,PKTn, a series of first offset values DELTA1,...,DELTAn and a series of second offset values GAMMA1,...,GAMMAk are received via a satellite link. A random number generation algorithm is employed to calculate and select one of the index numbers 1,...,n. The output of the random number generation algorithm is, for example the index 3. The packet whose index number was calculated, i.e. PKT3, is transmitted to the smart card.

In the smart card an algorithm which calculates seeds is employed to calculate the corresponding SEED3* number. SEED3* is then transmitted to descrambler unit 138.

The first offset value which corresponds to the calculated index number, i.e. DELTA3, is transmitted to the descrambling unit 138. A second offset value which identifies a supplier or jurisdiction, for example GAMMA2, is also transmitted to descrambler unit 138.

In the descrambler unit 138 SEED3*, DELTA3 and GAMMA2 are combined, by use of a secret number generation algorithm, to calculate a SEEDO value which is the secret number employed to descramble the satellite transmissions.

Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

Claims

1. A hacking prevention system for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number (SEED0) and when enabled being responsive to data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers comprising:

   a first key generator (36; 136), employing at least part of the data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) and a function (34; 134) which differs for at least a plurality of ones of the multiplicity of receivers, for generating a first key ($SEED_1$-$SEED_n$) which is different for each receiver having a different function; and
   a second key generator (32; 132) employing at least part of the data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) and the function (34; 134) to produce a second key ($DELTA_1$-$DELTA_n$);

   characterized in that the multiplicity of receivers further comprises:

   a secret number generator (38; 138) utilizing the first key ($SEED_1$-$SEED_n$) with the second key ($DELTA_1$-$DELTA_n$) to produce the secret number (SEED0) which is the same for all of the multiplicity of receivers,
   whereby first and second keys ($SEED_1$-$SEED_n$, $DELTA_1$-$DELTA_n$) intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

2. A hacking prevention system according to claim 1 wherein the function (34; 134) which differs for at least a plurality of ones of the multiplicity of receivers, is a random number generator (34; 134).

3. A hacking prevention system according to claims 1 or 2 wherein the second key generator (32; 132) is embodied in a single VLSI chip.

4. A hacking prevention system according to one or more of claims 1-3 wherein the first key generator (36; 136), a provider for the function (34; 134) and the secret number generator (38; 138) are embodied in a single VLSI chip.

5. A hacking prevention system according to one or more of claims 1-3 wherein the first key generator (36; 136), a provider for the function (34; 134), the secret number generator (38; 138) and the second key generator (32; 132) are embodied in a single VLSI chip.

6. A hacking prevention system according to one or more of claims 1-5 wherein each of the multiplicity of receivers comprises at least one of the VLSI chips.

7. A hacking prevention system according to one or more of claims 1-6 wherein the network is a CATV network and the multiplicity of receivers are CATV receivers and decoders.

8. A hacking prevention system according to one or more of claims 1-7 and also operative to selectively transmit information to the multiplicity of receivers from an information source, each of the multiplicity of receivers being associated with one of a multiplicity of subscribers which subscribers may be individually characterized by at least one of the following parameters: information suppliers, geographic locations, and demographics, and grouped into different groups according to at least one of the parameters, each of the multiplicity of receivers also comprising:

   a third key generator (132) employing at least part of the data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) to provide a third key ($GAMMA_1$-$GAMMA_k$) which is characterized by at least one of the parameters, wherein
   the secret number generator (38; 138) is operative to utilize the third key ($GAMMA_1$-$GAMMA_k$) with the first key ($SEED_1$-$SEED_n$) and the second key ($DELTA_1$-$DELTA_n$) to produce the secret number (SEED0) which is the same for all of the multiplicity of receivers, and
   the third key ($GAMMA_1$-$GAMMA_k$), when intercepted at a receiver which forms part of a first group of receivers being grouped according to at least one of the parameters, cannot be effective to enable a receiver which forms part of a second group of receivers being grouped according to at least one of the parameters.

9. A hacking prevention system acccording to one or more of claims 1-8 wherein the first key generator (36; 136) comprises:

   a packet receiver unit for receiving a data stream including at least a series of authorization packets (PKT_1-PKT_n),
   a packet provider for providing a selected packet, the selected packet being a packet whose serial number in the series of authorization packets (PKT_1-PKT_n) is equal to a random number integer in the range between one and the total number of packets in the series of authorization packets (PKT_1-PKT_n), the random

number integer being produced by the random number generator (34; 134), and
a first key receiver for receiving the first key ($SEED_1$-$SEED_n$) which uniquely corresponds to the selected packet.

10. A hacking prevention system according to claim 9 wherein the packet provider is operative to provide the selected packet to a removable smart card (36; 136), and the first key receiver is operative to receive the first key ($SEED_1$-$SEED_n$) from the removable smart card (36; 136).

11. A hacking prevention system according to one or more of claims 1-8 wherein the second key generator (32; 132) comprises:

an offset value receiver unit for receiving a data stream including at least a series of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) wherein each offset value in the series of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) is paired with a corresponding authorization packet in a series of authorization packets (PKT_1-PKT_n) ; and
an offset value provider for providing the second key ($DELTA_1$-$DELTA_n$), the second key ($DELTA_1$-$DELTA_n$) including at least an offset value which serial number in the series of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) is equal to a random number integer in the range between one and the total number of offset values in the series of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$), the random number integer being produced by the random number generator (34; 134).

12. A hacking prevention system according to claims 9 or 10 wherein the second key generator (32; 132) comprises:

an offset value receiver unit for receiving at least a set of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$), wherein each offset value in the series of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$ -$GAMMA_k$) is paired with a corresponding authorization packet in the series of authorization packets (PKT_1-PKT_n) ; and
an offset value provider for providing the second key ($DELTA_1$-$DELTA_n$), the second key ($DELTA_1$-$DELTA_n$) including at least an offset value which serial number in the series of offset values ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) is equal to the serial number of the selected packet.

13. A hacking prevention system according to one or more of claims 9, 10 and 12 wherein at least one of the first key generator (36; 136) and the secret number generator (38; 138) is embodied in at least one of a descrambler and a decrypter.

14. A hacking prevention method for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number (SEED0) and when enabled being responsive to data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) received from the transmitter for decrypting encrypted information, the method comprising the steps of:

generating a first key ($SEED_1$-$SEED_n$), by employing at least part of the data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) and a function (34; 134) which differs for at least a plurality of ones of the multiplicity of receivers, the first key ($SEED_1$-$SEED_n$) being different for each receiver having a different function; and
generating a second key ($DELTA_1$-$DELTA_n$) by employing at least part of the data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) and the function (34; 134),

characterized in that the method further comprises the steps of:

generating the secret number (SEED0) by utilizing the first key ($SEED_1$-$SEED_n$) with the second key ($DELTA_1$-$DELTA_n$) to produce the secret number (SEED0) which is the same for all of the multiplicity of receivers,
whereby first and second keys ($SEED_1$-$SEED_n$, $DELTA_1$-$DELTA_n$) intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

15. A method according to claim 14 and also comprising:

associating each of the multiplicity of receivers with one of a multiplicity of subscribers;
individually characterizing the multiplicity of subscribers by at least one of the following parameters: information suppliers, geographic locations, and demographics;
grouping the multiplicity of subscribers into different groups according to at least one of the parameters, the different groups being each selectively entitled to receive at least a portion of the information from an information source;
producing, at at least one of the multiplicity of receivers, a third key ($GAMMA_1$-$GAMMA_k$) by employing at least part of the data (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) to provide the third key ($GAMMA_1$-$GAMMA_k$) which is characterized by at least one of the parame-

ters, wherein
the step of generating the secret number (SEED0) comprises the step of generating the secret number (SEED0) which is the same for all of the multiplicity of receivers by utilizing the third key ($GAMMA_1$-$GAMMA_k$) with the first key and the second key ($SEED_1$-$SEED_n$, $DELTA_1$-$DELTA_n$), whereby
the third key ($GAMMA_1$-$GAMMA_k$), when intercepted at a receiver which forms part of a first group of receivers being grouped according to at least one of the parameters, cannot be effective to enable a receiver which forms part of a second group of receivers being grouped according to at least one of the parameters.

Patentansprüche

1. Ein Hackings-Verhinderungssystem zur Verwendung mit einem Netzwerk, das einen Sender und eine Vielzahl von Empfängern einschließt, wobei jeder Empfänger durch eine Geheimzahl (SEED0) unabhängig freigeschaltet wird, und sobald er freigeschaltet ist, auf Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) reagiert, die aus dem Sender empfangen werden, um eine verschlüsselte Information zu entschlüsseln, wobei jeder aus der Vielzahl von Empfängern folgendes umfaßt:

einen ersten Schlüssel-Generator (36; 136), der mindestens einen Teil der Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) und eine Funktion (34; 134) verwendet, die sich mindestens für eine Mehrzahl einiger aus der Vielzahl von Empfängern unterscheidet, um einen ersten Schlüssel (SEED1-SEEDn) zu erzeugen, der für jeden Empfänger, der über eine unterschiedliche Funktion verfügt, unterschiedlich ist; und
einen zweiten Schlüssel-Generator (32; 132), der mindestens einen Teil der Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) und die Funktion (34; 134) verwendet, um einen zweiten Schlüssel zu erzeugen (DELTA1-DELTAn);

dadurch gekennzeichnet, daß die Vielzahl von Empfängern weiterhin folgendes umfaßt:

einen Geheimzahl-Generator (38; 138), der den ersten Schlüssel (SEED1-SEEDn) mit dem zweiten Schlüssel (DELTA1-DELTAn) verwendet, um die Geheimzahl zu erzeugen, die für alle der Vielzahl von Empfängern dieselbe ist, wodurch der erste und der zweite Schlüssel (SEED1-SEEDn, DELTA1-DELTAn), die an einem ersten Empfänger abgefangen werden, nicht wirksam sein können, um einen zweiten Empfänger, der eine unterschiedliche Funktion aufweist, freizuschalten.

2. Ein Hackings-Verhinderungssystem nach Anspruch 1, worin die Funktion (34; 134), die sich für mindestens eine Mehrzahl einiger aus der Vielzahl von Empfängern unterscheidet, ein Zufallszahl-Generator (34; 134) ist.

3. Ein Hackings-Verhinderungssystem nach den Ansprüchen 1 oder 2, worin der zweite Schlüssel-Generator (32; 132) auf einem einzigem VLSI-Chip ausgebildet ist

4. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-3, worin der erste Schlüssel-Generator (36; 136), ein Bereitsteller für die Funktion (34; 134) und der Geheimzahl-Generator (38; 138) auf einem einzigen VLSI-Chip ausgebildet sind.

5. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-3, worin der erste Schlüssel-Generator (36; 136), ein Bereitsteller für die Funktion (34; 134), der Geheimzahl-Generator (38; 138) und der zweite Schlüssel-Generator (32; 132) auf einem einzigen VLSI-Chip ausgebildet sind.

6. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-5, worin jeder der Vielzahl von Empfängern mindestens einen der VLSI-Chips umfaßt.

7. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-6, worin das Netzwerk ein Kabelfernseh-Netzwerk ist und die Vielzahl an Empfängern Kabelfernseh-Empfänger und -Dekodierer sind.

8. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-7, das ebenfalls betriebsfähig ist, um aus einer Informationsquelle der Vielzahl von Empfängern selektiv eine Information zuzusenden, wobei jeder der Vielzahl von Empfängern mit einem Teilnehmer aus einer Vielzahl von Teilnehmern assoziiert ist, wobei diese Teilnehmer einzeln durch mindestens einen der folgenden Parameter gekennzeichnet sein können: Informationslieferanten, geographische Lagen und Bevölkerungszahlstatistiken; und die gemäß mindestens einem dieser Parameter in unterschiedliche Gruppen unterteilt werden, wobei jeder der Vielzahl von Empfängern ebenso folgendes umfaßt:

einen dritten Schlüssel-Generator (132), der

mindestens einen Teil der Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) verwendet, um einen dritten Schlüssel (GAMMA1-GAMMAk) bereitzustellen, der durch mindestens einen der Parameter gekennzeichnet ist, worin
der Geheimzahl-Generator (38; 138) betriebsfähig ist, um den dritten Schlüssel (GAMMA1-GAMMAk) mit dem ersten Schlüssel (SEED1-SEEDn) und mit dem zweiten Schlüssel (DELTA1-DELTAn) zu verwenden, um die Geheimzahl (SEED0) zu erzeugen, die für alle der Vielzahl von Empfängern dieselbe ist, und worin
der dritte Schlüssel (GAMMA1-GAMMAk), sobald er an einem Empfänger abgefangen wird, der Teil einer ersten Gruppe von Empfängern bildet, die in Übereinstimmung mit mindestens einem der Parameter unterteilt sind, nicht wirksam sein kann, um einen Empfänger freizuschalten, der Teil einer zweiten Gruppe von Empfängern bildet, die in Übereinstimmung mit mindestens einem der Parameter unterteilt sind.

9. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-8, worin der erste Schlüssel-Generator (36; 136) folgendes umfaßt:

eine Datenpacket-Empfängereinheit zum Empfangen eines Datenstroms, der mindestens eine Reihe von Berechtigungs-Datenpacketen (PKT1-PKTn) einschließt,
einen Datenpacket-Bereitsteller zum Bereitstellen eines ausgewählten Datenpackets, wobei das ausgewählte Datenpacket ein Datenpacket ist, dessen Seriennummer in der Reihe von Berechtigungs-Datenpacketen (PKT1-PKTn) gleich einer ganzzahligen Zufallszahl ist, die im Bereich zwischen eins und der Gesamtzahl von Datenpacketen in der Reihe von Berechtigungs-Datenpacketen (PKT1-PKTn) liegt, wobei die ganzzahlige Zufallszahl durch den Zufallszahl-Generator (34; 134) erzeugt wird, und
einen ersten Schlüsselempfänger, um den ersten Schlüssel (SEED1-SEEDn) zu empfangen, der eindeutig dem ausgewählten Datenpacket entspricht.

10. Ein Hackings-Verhinderungssystem nach Anspruch 9, worin der Datenpacket-Bereitsteller betriebsfähig ist, um das ausgewählte Datenpacket einer entfernbaren Chip-Karte (36; 136) bereitzustellen, und worin der erste Schlüsselempfänger betriebsfähig ist, um den ersten Schlüssel (SEED1-SEEDn) aus der entfernbaren Chip-Karte (36; 136) zu empfangen.

11. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 1-8, worin der zweite Schlüssel-Generator (32; 132) folgendes umfaßt:

eine Offset-Wert-Empfängereinheit zum Empfangen eines Datenstroms, der mindestens eine Reihe von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk) einschließt, worin jeder Offset-Wert in den Reihen von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk) mit einem entsprechenden Berechtigungs-Datenpacket in der Reihe von Berechtigungs-Datenpacketen (PKT1-PKTn) gepaart ist; und
einen Offset-Wert-Bereitsteller zum Bereitstellen des zweiten Schlüssels (DELTA1-DELTAn), wobei der zweite Schlüssel (DELTA1-DELTAn) mindestens einen Offset-Wert einschließt, dessen Seriennummer in der Reihe von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk) gleich einer ganzzahligen Zufallszahl ist, die im Bereich zwischen eins und der Gesamtzahl an Offset-Werten in der Reihe von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk) liegt, wobei die ganzzahlige Zufallszahl vom Zufallszahl-Generator (34; 134) erzeugt wird.

12. Ein Hackings-Verhinderungssystem nach Anspruch 9 oder 10, worin der zweite Schlüssel-Generator (32; 132) folgendes umfaßt:

eine Offset-Wert-Empfängereinheit zum Empfangen von mindestens einem Satz von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk), worin jeder Offset-Wert in den Reihen von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk) mit einem entsprechenden Berechtigungs-Datenpacket in der Reihe von Berechtigungs-Datenpacketen (PKT1-PKTn) gepaart ist; und
einen Offset-Wert-Bereitsteller zum Bereitstellen des zweiten Schlüssels (DELTA1-DELTAn), wobei der zweite Schlüssel (DELTA1-DELTAn) mindestens einen Offset-Wert einschließt, dessen Seriennummer in der Reihe von Offset-Werten (DELTA1-DELTAn, GAMMA1-GAMMAk) gleich mit der Seriennummer des ausgewählten Datenpackets ist.

13. Ein Hackings-Verhinderungssystem nach einem oder mehreren der Ansprüche 9, 10 und 12, worin mindestens einer des ersten Schlüssel-Generators (36; 136) oder des Geheimzahl-Generators (38; 138) in mindestens einem eines Zerhacker oder eines Dekodierers ausgebildet ist.

14. Ein Hackings-Verhinderungsverfahren zur Verwendung mit einem Netzwerk, das einen Sender und

eine Vielzahl von Empfängern einschließt, wobei jeder Empfänger unabhängig von einer Geheimzahl (SEED0) freigeschaltet wird, und sobald er freigeschaltet ist, auf Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) reagiert, die aus dem Sender empfangen werden, um eine verschlüsselte Information zu entschlüsseln, wobei das Verfahren die folgenden Schritte umfaßt:

das Erzeugen eines ersten Schlüssels (SEED1-SEEDn), indem mindestens ein Teil der Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) und eine Funktion (34; 134) verwendet wird, die sich mindestens für eine Mehrzahl einiger aus der Vielzahl von Empfängern unterscheidet, wobei der erste Schlüssel (SEED1-SEED0) für jeden Empfänger unterschiedlich ist, der über eine unterschiedliche Funktion verfügt; und
das Erzeugen eines zweiten Schlüssels (DELTA1-DELTAn), indem mindestens ein Teil der Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) und die Funktion (34; 134) verwendet wird, dadurch gekennzeichnet, daß das Verfahren weiterhin die folgenden Schritte umfaßt:
das Erzeugen der Geheimzahl (SEED0), indem der erste Schlüssel (SEED1-SEEDn) mit dem zweiten Schlüssel (DELTA1-DELTAn) verwendet wird, um die Geheimzahl (SEED0) zu erzeugen, die für alle aus der Vielzahl von Empfängern dieselbe ist,
wodurch der erste und der zweite Schlüssel (SEED1-SEEDn, DELTA1-DELTAn), die an einem ersten Empfänger abgefangen werden, nicht wirksam sein können, um einen zweiten Empfänger, der eine unterschiedliche Funktion aufweist, freizuschalten.

15. Ein Verfahren nach Anspruch 14, das ebenfalls folgendes umfaßt:

das Assoziieren eines jeden aus der Vielzahl von Empfängern mit einem Teilnehmer aus einer Vielzahl von Teilnehmern;
die einzelne Kennzeichnung der Vielzahl von Teilnehmern durch mindestens einen der folgenden Parameter: Informationslieferanten, geographischen Lagen und Bevökerungszahlstatistiken;
das Unterteilen der Vielzahl von Teilnehmern in verschiedene Gruppen, und zwar in Übereinstimmung mit mindestens einem der Parameter, wobei die verschiedenen Gruppen alle selektiv berechtigt werden, um mindestens einen Teil der Information aus einer Informationsquelle zu empfangen;
das Erzeugen eines dritten Schlüssels (GAMMA1-GAMMAk) an mindestens einem aus der Vielzahl von Empfängern, indem mindestens ein Teil der Daten (PKT1-PKTn, DELTA1-DELTAn, GAMMA1-GAMMAk) verwendet wird, um den dritten Schlüssel (GAMMA1-GAMMAk) bereitzustellen, der durch mindestens einen der Parameter gekennzeichnet ist, worin
der Schritt zum Erzeugen der Geheimzahl (SEED0) den Schritt zum Erzeugen der Geheimzahl (SEED0) umfaßt, die für alle aus der Vielzahl von Empfängern dieselbe ist, und zwar indem der dritte Schlüssel (GAMMA1-GAMMAk) mit dem ersten Schlüssel und mit dem zweiten Schlüssel (SEED1-SEEDn, DELTA1-DELTAn) verwendet wird, wodurch
der dritte Schlüssel (GAMMA1-GAMMAk), sobald er am Empfänger abgefangen wird, der Teil einer ersten Gruppe von Empfängern bildet, die in Übereinstimmung mit mindestens einem der Parameter unterteilt werden, nicht wirksam sein kann, um einen Empfänger freizuschalten, der Teil einer zweiten Gruppe von Empfängern bildet, die in Übereinstimmung mit mindestens einem der Parameter unterteilt werden.

Revendications

1. Système de prévention du piratage à utiliser avec un réseau comprenant un émetteur et une pluralité de récepteurs, chaque récepteur étant validé indépendamment par un code secret (SEED0) et réagissant, lorsqu'il est validé, à des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) reçues de l'émetteur pour déchiffrer une information chiffrée, chacun de la pluralité de récepteurs comprenant :

un premier générateur de clé (36; 136), utilisant au moins une partie des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) et une fonction (34; 134) qui diffère pour au moins une pluralité de récepteurs de la pluralité de récepteurs, pour générer une première clé ($SEED_1$-$SEED_n$) qui est différente pour chaque récepteur ayant une fonction différente; et
un deuxième générateur de clé (32; 132) utilisant au moins une partie des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) et la fonction (34; 134) pour produire une deuxième clé ($DELTA_1$-$DELTA_n$);

caractérisé en ce que la pluralité de récepteurs comprend de plus :

un générateur de code secret (38; 138) utilisant

la première clé ($SEED_1$-$SEED_n$) avec la deuxième clé ($DELTA_1$-$DELTA_n$) pour produire le code secret (SEED0) qui est le même pour tous les récepteurs de la pluralité de récepteurs,
la première et la deuxième clés ($SEED_1$-$SEED_n$, $DELTA_1$-$DELTA_n$), interceptées à un premier récepteur ne pouvant pas valider un deuxième récepteur ayant une fonction différente.

2. Système de prévention de piratage selon la revendication 1 dans lequel la fonction (34; 134) qui diffère pour au moins une pluralité de récepteurs de la pluralité de récepteurs, est un générateur de nombre aléatoire (34; 134).

3. Système de prévention de piratage selon les revendications 1 ou 2 dans lequel le deuxième générateur de clé (32; 132) est réalisé dans une puce ITGE unique.

4. Système de prévention de piratage selon une ou plusieurs des revendications 1-3 dans lequel le premier générateur de clé (36; 136), un fournisseur pour la fonction (34; 134) et le générateur de code secret (38; 138) sont réalisés dans une puce ITGE unique.

5. Système de prévention de piratage selon une ou plusieurs des revendications 1-3 dans lequel le premier générateur de clé (36; 136), un fournisseur pour la fonction (34; 134), le générateur de code secret (38; 138) et le deuxième générateur de clé (32; 132) sont réalisés dans une puce ITGE unique.

6. Système de prévention de piratage selon une ou plusieurs des revendications 1-5 dans lequel chacun de la pluralité de récepteurs comprend au moins une des puces ITGE.

7. Système de prévention de piratage selon une ou plusieurs des revendications 1-6 dans lequel le réseau est un réseau CATV et la pluralité de récepteurs sont des récepteurs et des décodeurs CATV.

8. Système de prévention de piratage selon une ou plusieurs des revendications 1-7 et pouvant également transmettre sélectivement des informations à la pluralité de récepteurs d'un émetteur d'informations, chacun de la pluralité de récepteurs étant associé à l'un d'une pluralité d'abonnés, lesquels abonnés peuvent être individuellement caractérisés par au moins un des paramètres suivants : fournisseurs d'information, emplacements géographiques, et démographie, et groupés dans différents groupes selon au moins un des paramètres, chacun de la pluralité de récepteurs comprenant également :

un troisième générateur de clé (132) utilisant au moins une partie des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) pour fournir une troisième clé ($GAMMA_1$-$GAMMA_k$) qui se caractérise par au moins un des paramètres, dans lequel
le générateur de code secret (38; 138) sert à utiliser la troisième clé ($GAMMA_1$-$GAMMA_k$) avec la première clé ($SEED_1$-$SEED_n$) et la deuxième clé ($DELTA_1$-$DELTA_n$) pour produire le code secret (SEED0) qui est le même pour toute la pluralité de récepteurs, et
la troisième clé ($GAMMA_1$-$GAMMA_k$), lorsqu'elle est interceptée à un récepteur qui fait partie d'un premier groupe de récepteurs groupés selon au moins un des paramètres, ne peut pas valider un récepteur qui fait partie d'un deuxième groupe de récepteurs groupés selon au moins un des paramètres.

9. Système de prévention de piratage selon une ou plusieurs des revendications 1-8 dans lequel le premier générateur de clé (36; 136) comprend :

une unité de récepteur de paquet pour recevoir un flux de données comprenant au moins une série de paquets d'autorisation (PKT_1-PKT_n),
un fournisseur de paquet pour fournir un paquet choisi, le paquet choisi étant un paquet dont le numéro de série dans la série de paquets d'autorisation (PKT_1-PKT_n) est égal à un nombre entier aléatoire compris dans l'intervalle allant de un au nombre total de paquets dans la série de paquets d'autorisation (PKT_1-PKT_n), le nombre entier aléatoire étant produit par le générateur de nombre aléatoire (34; 134), et
un premier récepteur de clé pour recevoir la première clé ($SEED_1$-$SEED_n$) qui correspond uniquement au paquet choisi.

10. Système de prévention de piratage selon la revendication 9 dans lequel le fournisseur de paquet sert à fournir le paquet choisi à une carte à mémoire amovible (36; 136), et le premier récepteur de clé sert à recevoir la première clé ($SEED_1$-$SEED_n$) de la carte à mémoire amovible (36; 136).

11. Système de prévention de piratage selon une ou plusieurs des revendications 1-8 dans lequel le deuxième générateur de clé (32; 132) comprend :

une unité de récepteur de valeur de décalage pour recevoir un flux de données comprenant au moins une série de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) dans lequel chaque valeur de décalage de la série

de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) est appariée à un paquet d'autorisation correspondant dans une série de paquets d'autorisation (PKT_1-PKT_n); et
un fournisseur de valeur de décalage pour fournir la deuxième clé ($DELTA_1$-$DELTA_n$), la deuxième clé ($DELTA_1$-$DELTA_n$) comprenant au moins une valeur de décalage dont le numéro de série dans la série de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) est égal à un nombre entier aléatoire compris dans l'intervalle allant de un au nombre de valeurs de décalage dans la série de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$), le nombre entier aléatoire étant produit par le générateur de nombre aléatoire (34; 134).

12. Système de prévention de piratage selon les revendications 9 ou 10 dans lequel le deuxième générateur de clé (32; 132) comprend :

une unité de récepteur de valeur de décalage pour recevoir au moins un ensemble de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$), dans lequel chaque valeur de décalage de la série de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) est appariée à un paquet d'autorisation correspondant de la série de paquets d'autorisation (PKT_1-PKT_n); et
un fournisseur de valeur de décalage pour fournir la deuxième clé ($DELTA_1$-$DELTA_n$), la deuxième clé ($DELTA_1$-$DELTA_n$), comprenant au moins une valeur de décalage dont le numéro de série dans la série de valeurs de décalage ($DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) est égal au numéro de série du paquet choisi.

13. Système de prévention de piratage selon une ou plusieurs des revendications 9, 10 et 12 dans lequel l'un au moins du premier générateur de clé (36; 136) et du générateur de code secret (38; 138) est mis en oeuvre dans l'un au moins d'un désembrouilleur et d'un déchiffreur.

14. Procédé de prévention de piratage destiné à être utilisé avec un réseau comprenant un émetteur et une pluralité de récepteurs, chaque récepteur étant validé indépendamment par un code secret (SEED0) et étant sensible, lorsqu'il est validé, à des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) reçues de l'émetteur pour déchiffrer une information chiffrée, le procédé comprenant les opérations consistant à :

générer une première clé ($SEED_1$-$SEED_n$), en utilisant au moins une partie des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) et une fonction (34; 134) qui diffère pour au moins une pluralité de récepteurs de la pluralité de récepteurs, la première clé ($SEED_1$-$SEED_n$) étant différente pour chaque récepteur ayant une fonction différente; et
générer une deuxième clé ($DELTA_1$-$DELTA_n$) en utilisant au moins une partie des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) et la fonction (34; 134),

caractérisé en ce que le procédé comprend de plus les opérations consistant à :

générer le code secret (SEED0) en utilisant la première clé ($SEED_1$-$SEED_n$) avec la deuxième clé ($DELTA_1$-$DELTA_n$) pour produire le code secret (SEED0) qui est le même pour tous les récepteurs de la pluralité de récepteurs,
la première et la deuxième clés ($SEED_1$-$SEED_n$, $DELTA_1$-$DELTA_n$) interceptées à un premier récepteur ne pouvant pas valider un deuxième récepteur ayant une fonction différente.

15. Procédé selon la revendication 14 et comprenant également les opérations consistant à :

associer chacun de la pluralité de récepteurs à l'un d'une pluralité d'abonnés;

caractériser individuellement la pluralité d'abonnés par au moins un des paramètres suivants : fournisseurs de l'information, emplacements géographiques, et démographie;

grouper la pluralité d'abonnés dans différents groupes selon au moins un des paramètres, les différents groupes étant chacun sélectivement autorisé à recevoir au moins une partie de l'information provenant d'un émetteur d'informations;
produire, en au moins un de la pluralité de récepteurs, une troisième clé ($GAMMA_1$-$GAMMA_k$) en utilisant au moins une partie des données (PKT_1-PKT_n, $DELTA_1$-$DELTA_n$, $GAMMA_1$-$GAMMA_k$) pour fournir la troisième clé ($GAMMA_1$-$GAMMA_k$) qui est caractérisée par au moins un des paramètres,
l'opération consistant à générer le code secret (SEED0) comprenant l'opération consistant à générer le code secret (SEED0) qui est le même pour toute la pluralité de récepteurs en utilisant la troisième clé ($GAMMA_1$-$GAMMA_k$) avec la première clé et la deuxième clé ($SEED_1$-$SEED_n$, $DELTA_1$-$DELTA_n$),
la troisième clé ($GAMMA_1$-$GAMMA_k$), lorsqu'elle est interceptée à un récepteur qui fait

partie d'un premier groupe de récepteurs groupés selon au moins un des paramètres, ne pouvant pas valider un récepteur qui fait partie d'un deuxième groupe de récepteurs groupés selon au moins un des paramètres.

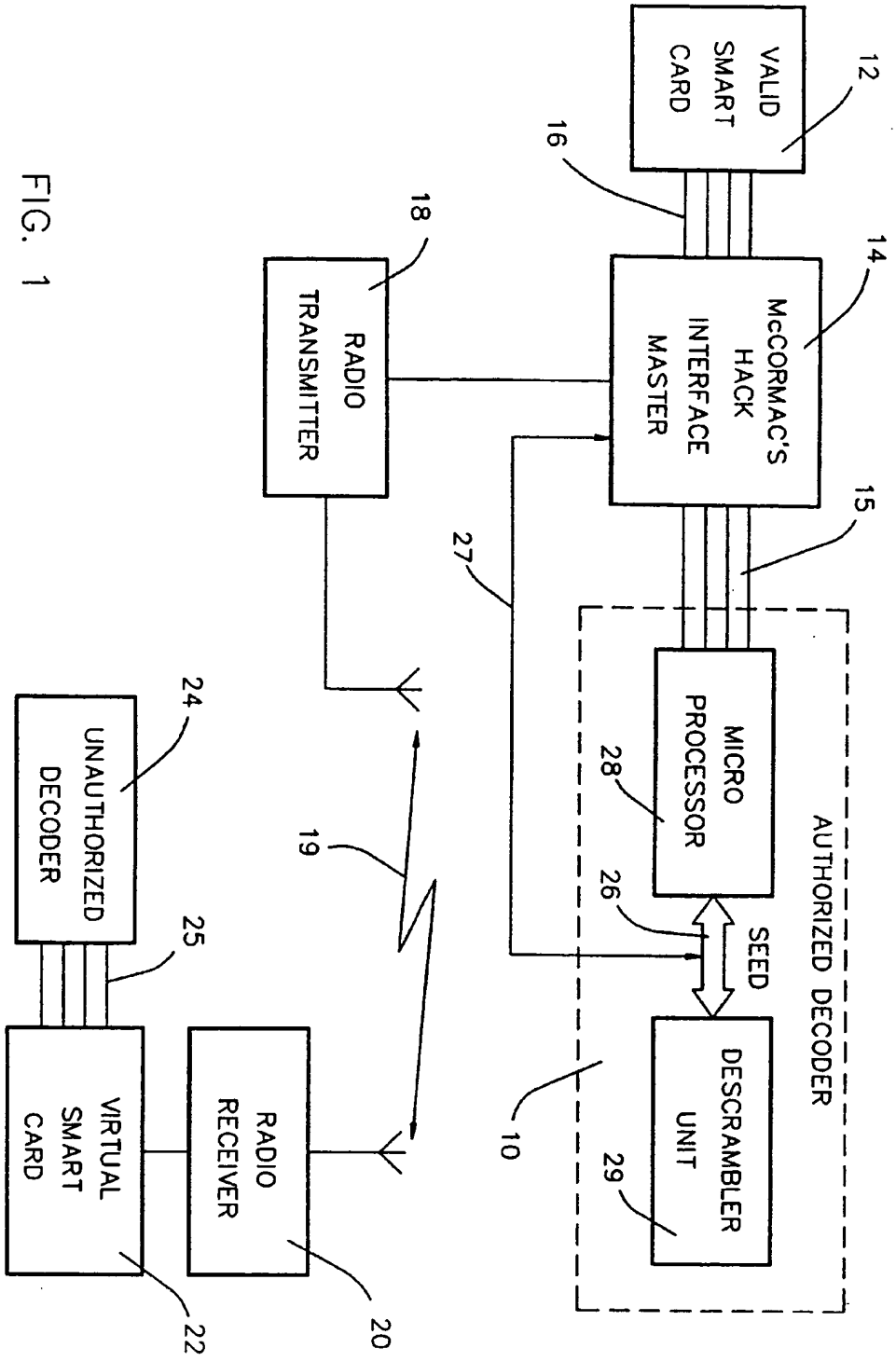
VALID SMART CARD
12
16
McCORMAC'S HACK INTERFACE MASTER
14
18
RADIO TRANSMITTER
15
27
AUTHORIZED DECODER
MICRO PROCESSOR
28
26
SEED
DESCRAMBLER UNIT
29
10
19
24
UNAUTHORIZED DECODER
25
VIRTUAL SMART CARD
22
RADIO RECEIVER
20

FIG. 1

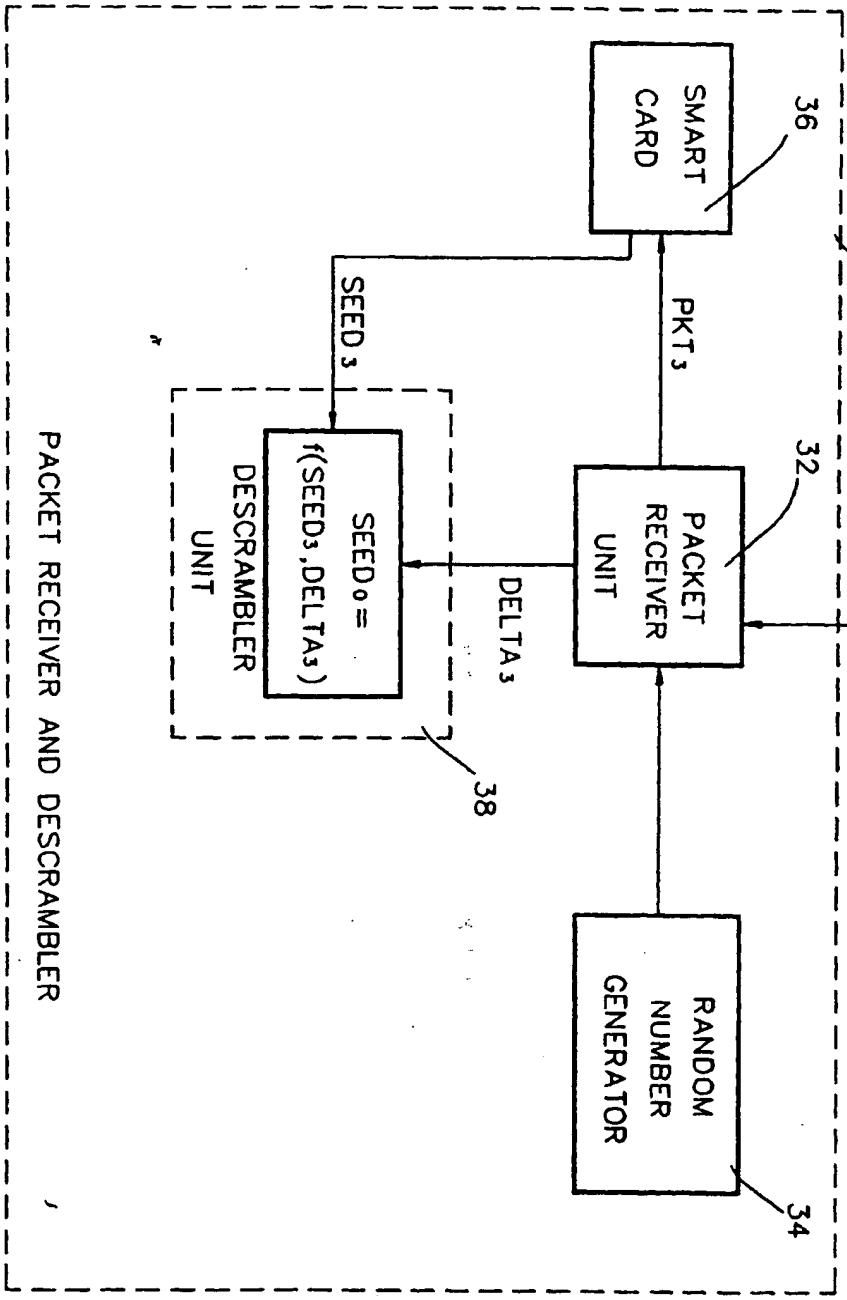
PACKET RECEIVER AND DESCRAMBLER
30
SMART CARD
36
PKT 3
SEED 3
PACKET RECEIVER UNIT
32
PKT1,... PKTn AND DELTA1,... DELTAn FROM SATELLITE LINK
DELTA 3
SEED0 = f(SEED3,DELTA3)
DESCRAMBLER UNIT
38
RANDOM NUMBER GENERATOR
34

FIG. 2

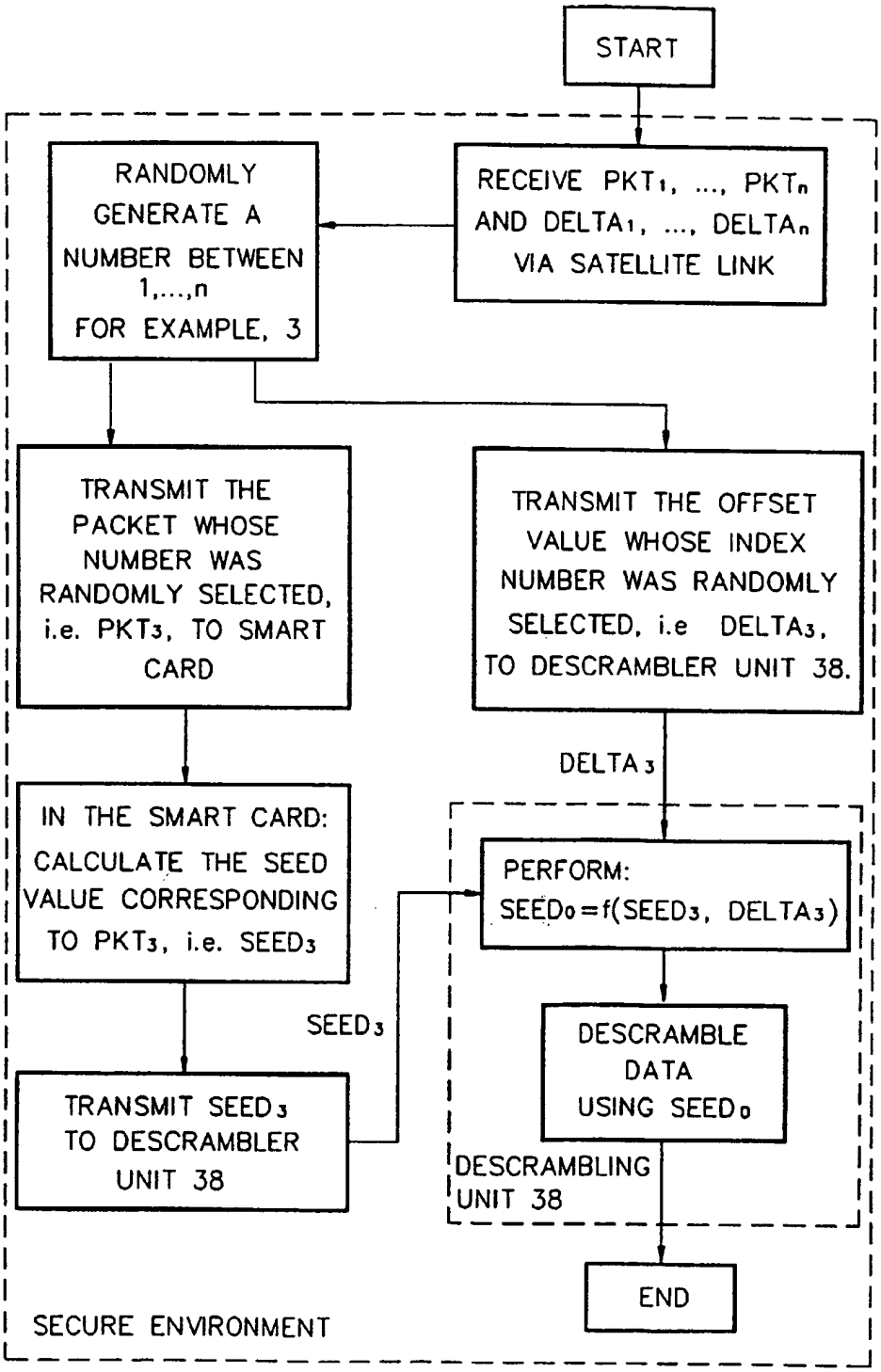
START
RANDOMLY GENERATE A NUMBER BETWEEN 1,...,n FOR EXAMPLE, 3
RECEIVE PKT1, ..., PKTn AND DELTA1, ..., DELTAn VIA SATELLITE LINK
TRANSMIT THE PACKET WHOSE NUMBER WAS RANDOMLY SELECTED, i.e. PKT3, TO SMART CARD
TRANSMIT THE OFFSET VALUE WHOSE INDEX NUMBER WAS RANDOMLY SELECTED, i.e DELTA3, TO DESCRAMBLER UNIT 38.
DELTA3
IN THE SMART CARD: CALCULATE THE SEED VALUE CORRESPONDING TO PKT3, i.e. SEED3
PERFORM: SEED0=f(SEED3, DELTA3)
SEED3
DESCRAMBLE DATA USING SEED0
TRANSMIT SEED3 TO DESCRAMBLER UNIT 38
DESCRAMBLING UNIT 38
END
SECURE ENVIRONMENT

FIG. 3

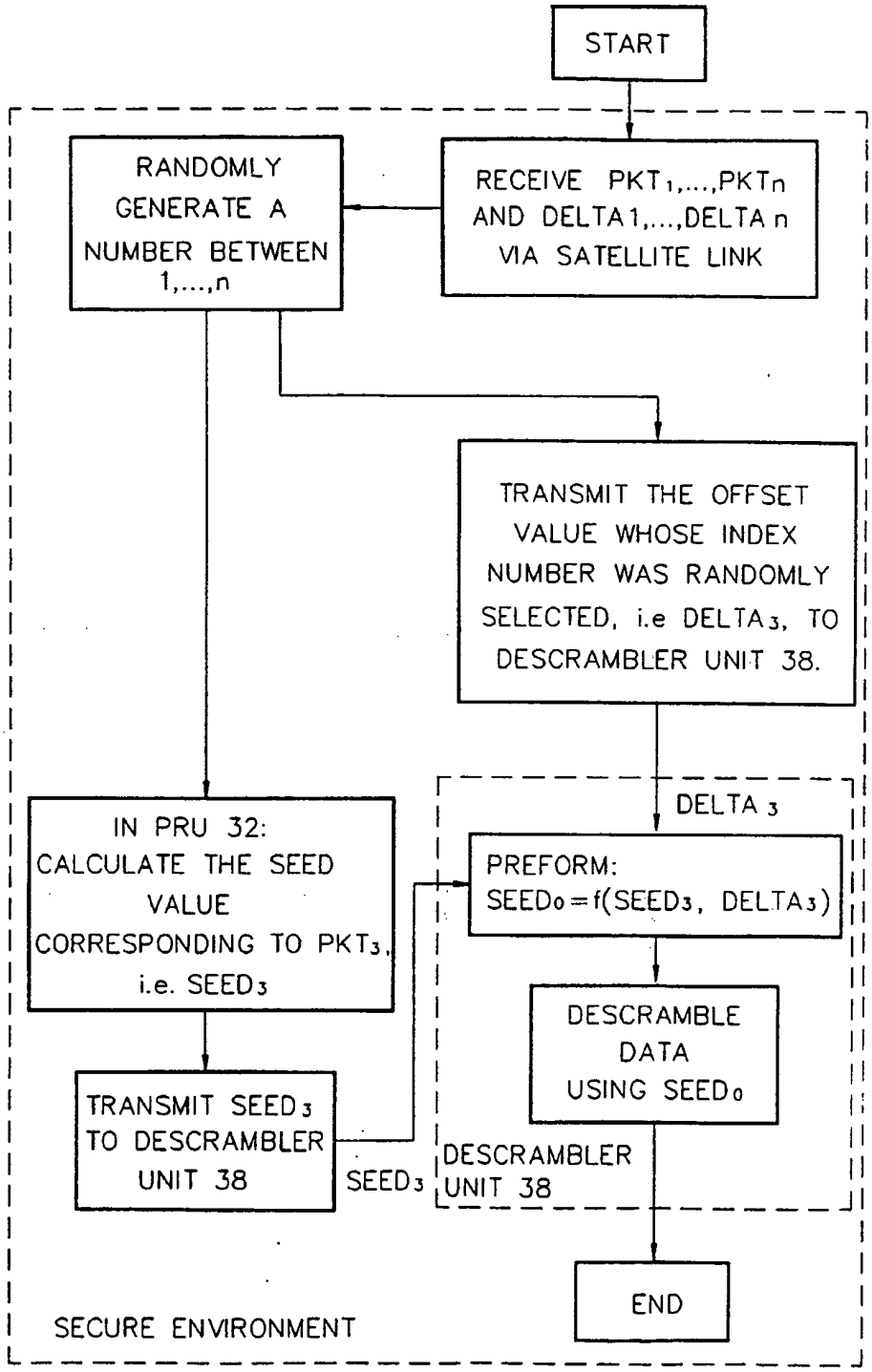
START
RANDOMLY GENERATE A NUMBER BETWEEN 1,...,n
RECEIVE PKT1,...,PKTn AND DELTA1,...,DELTA n VIA SATELLITE LINK
TRANSMIT THE OFFSET VALUE WHOSE INDEX NUMBER WAS RANDOMLY SELECTED, i.e DELTA3, TO DESCRAMBLER UNIT 38.
DELTA 3
IN PRU 32: CALCULATE THE SEED VALUE CORRESPONDING TO PKT3, i.e. SEED3
PREFORM: SEED0 = f(SEED3, DELTA3)
DESCRAMBLE DATA USING SEED0
TRANSMIT SEED3 TO DESCRAMBLER UNIT 38
SEED3
DESCRAMBLER UNIT 38
END
SECURE ENVIRONMENT

FIG. 4

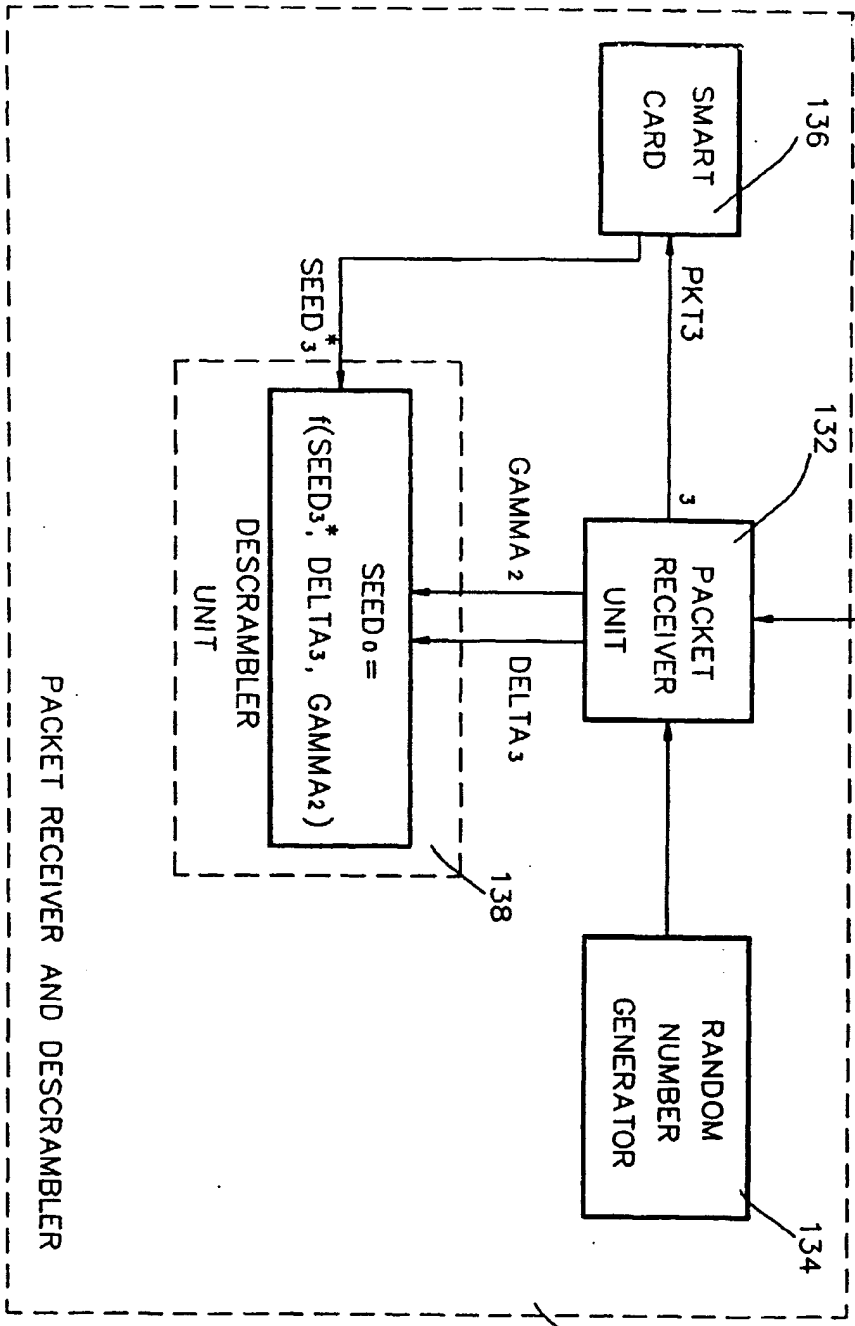
PKT1,..., PKTn, DELTA1,..., DELTAn AND GAMMA1,..., GAMMAk
FROM SATELLITE LINK
SMART CARD
136
PKT3
SEED*3
132
PACKET RECEIVER UNIT
GAMMA 2
DELTA 3
SEED0 = f(SEED3*, DELTA3, GAMMA2)
DESCRAMBLER UNIT
138
RANDOM NUMBER GENERATOR
134
130
PACKET RECEIVER AND DESCRAMBLER

FIG. 5

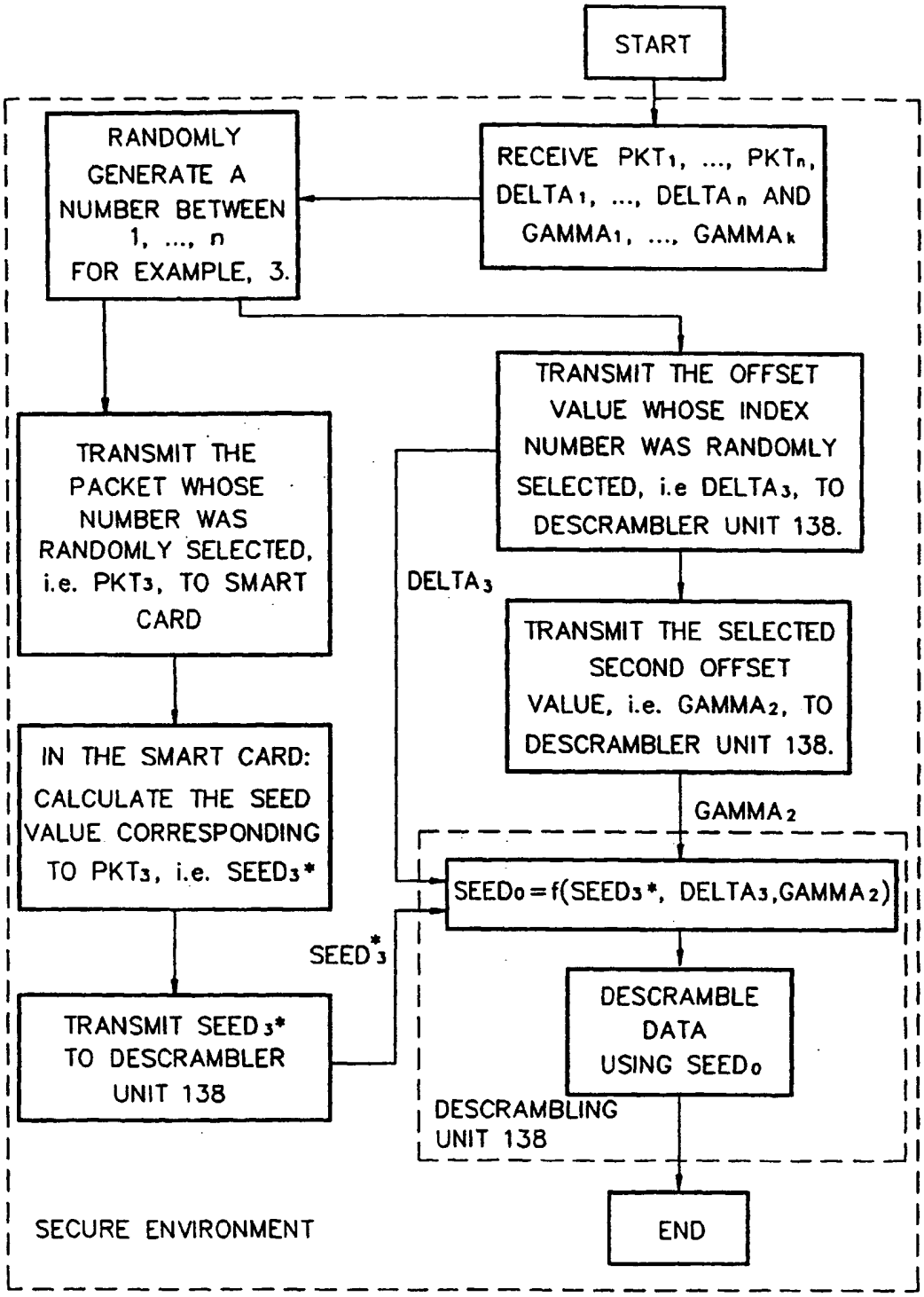
START
RANDOMLY GENERATE A NUMBER BETWEEN 1, ..., n FOR EXAMPLE, 3.
RECEIVE PKT1, ..., PKTn, DELTA1, ..., DELTAn AND GAMMA1, ..., GAMMAk
TRANSMIT THE OFFSET VALUE WHOSE INDEX NUMBER WAS RANDOMLY SELECTED, i.e DELTA3, TO DESCRAMBLER UNIT 138.
TRANSMIT THE PACKET WHOSE NUMBER WAS RANDOMLY SELECTED, i.e. PKT3, TO SMART CARD
DELTA3
TRANSMIT THE SELECTED SECOND OFFSET VALUE, i.e. GAMMA2, TO DESCRAMBLER UNIT 138.
GAMMA2
IN THE SMART CARD: CALCULATE THE SEED VALUE CORRESPONDING TO PKT3, i.e. SEED3*
SEED0=f(SEED3*, DELTA3,GAMMA2)
SEED*3
DESCRAMBLE DATA USING SEED0
TRANSMIT SEED3* TO DESCRAMBLER UNIT 138
DESCRAMBLING UNIT 138
SECURE ENVIRONMENT
END

FIG. 6